

# A Quick Tour of a SekChek Report: 1 of 8

## An overall rating of your system's security controls...

**Security Analysis: World Communication**  
System: ZEUS (olympus.com)  
Analysis Date: 20-Oct-2009 CONFIDENTIAL

**Rating Against Industry Average**

☺	☹	☹
X		

**Overall Comments**

Overall, security is above average compared with other Windows Domain Controllers running Active Directory used in the Communications sector.

The administrator should consider changing the password for those accounts with Administrative Authority on a regular basis.

The machine does not have the latest Service Pack for Windows installed. The latest is SP2.

**Report Highlights**

Report Section	Comments
3	System Policy settings are generally OK. However, <ul style="list-style-type: none"><li>The client could consider renaming the Administrator and Guest accounts.</li></ul>

SekChek's reports provide a convenient, objective and consistent assessment of your organisation's security controls in a format that is easy to read and interpret.

Assessments, which are based on your particular industry sector, compare and benchmark your security against dynamic, real-life industry averages and leading practices for security.

The picture shows the optional summary document available with the SekChek Classic service. The document provides you with a consultant's overall rating against your industry peers that use systems of a similar size and technology.

SekChek's analyses include several layers of reporting designed for different audiences:

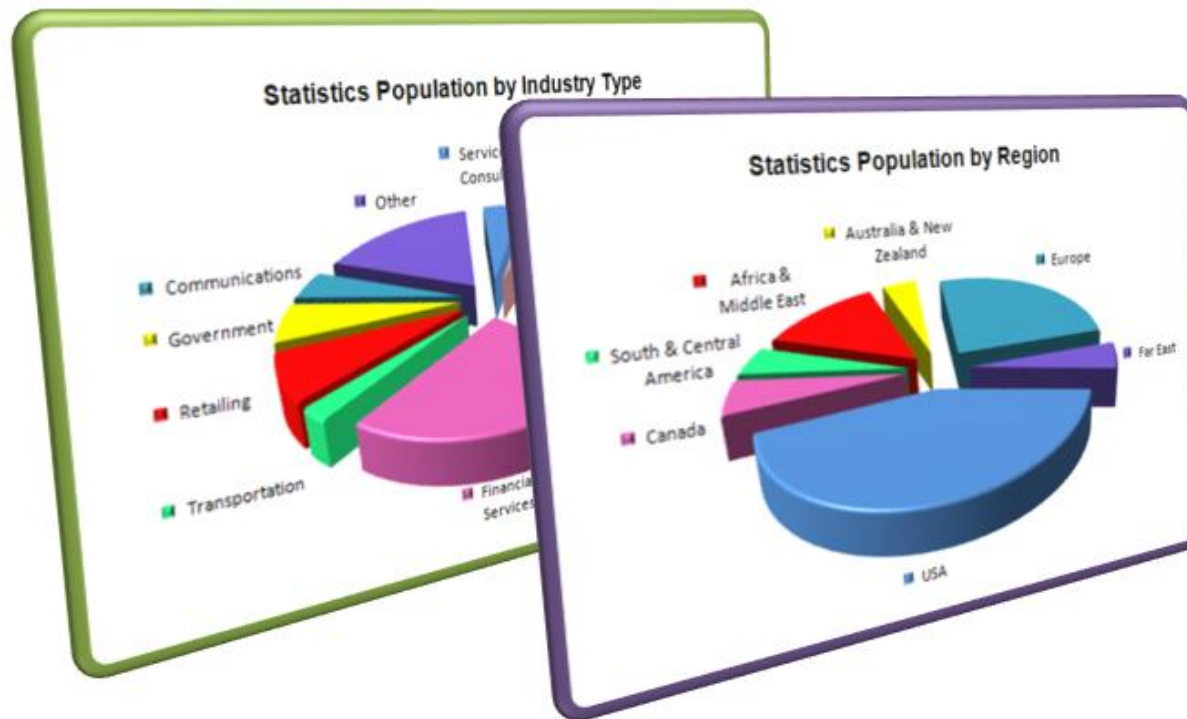
- An overall rating, graphical and text-based summaries for senior, non-technical management. These reports provide a perspective on how your security ranks against your industry peers and help you to quickly determine whether security is improving or weakening over time.
- Comprehensive exception reports with implications, risk ratings and recommended actions for technical personnel responsible for correcting highlighted weaknesses in controls.

This rich collection of data provides you with a clear view of how your security compares against real-life averages and leading practices in your particular industry sector.

SekChek benchmarks your security against a rich and ever-changing database of anonymous security data, categorised by industry sector, geographical region, computer platform and system size.

## A Quick Tour of a SekChek Report: 2 of 8

### *Benchmarking against real-life industry averages and leading practices for security...*



SekChek's unique and dynamic statistics database contains more than 30 million individual security measurements compiled over 10 years from:

- More than 60,000 computer systems and domains...
- Running MS-Windows, Active Directory, OS/400, UNIX and Novell / Netware...
- Located in more than 110 countries and used in...
- 22 industry sectors.

SekChek reports support and measure the efforts of professionals in internal audit, external audit and information security.

They also reduce the cost and burden of compliance with industry specific legislation.

# A Quick Tour of a SekChek Report: 3 of 8

*More than 40 detailed report sections...*

Table of Contents		
SekChek Options		
System Details		
System Configuration		
1. Report Summary		
1.1 Comparisons Against		
1.2 Summary of Changes		
2. Domain Structure		
3. Domain Accounts Policy		
4. Domain Controller Policy		
4.1 Audit Policy Settings		
4.2 Event log Settings		
4.3 Security Option Setting		
5. Group Policy Objects		
5.1 Description and Properties		
5.2 Summary of GPOs defined		
5.3 Summary of GPOs and their		
5.4 Summary of OUs and their		
5.5 GPOs Defined and their		
6. Customer-Selected Registry Key Values	54	
7. User Accounts Defined in The Domain	55	
8. Groups Defined in the Domain	58	
9. Domain Local Groups and their Members	62	
10. Domain Global Groups and their Members	65	
11. Domain Universal Groups	68	
12. Last Logons, 30 Days and		
13. Passwords, 30 Days and		
14. Passwords that Never Expire		
15. Accounts not Requiring a		
16. Invalid Logon Attempts G		
17. Accounts with Expiry Date		
18. Disabled Accounts		
19. Locked Out Accounts		
20. Accounts Whose Passwords		
21. Rights and Privileges		
21.1 Descriptions & General		
21.2 Rights Assigned to Local		
21.3 Rights Assigned to Universal		
21.4 Rights Assigned to Global		
21.5 Rights Assigned to Users	96	
21.6 Rights Assigned to Well-Known Objects	100	
21.7 Rights Assigned to External Objects	101	
22. Discretionary Access Controls (DACL) for Containers	111	
23. Trusted and Trusting Domains	115	
24. Servers and Workstations	116	
25. Domain Controllers in the Domain	118	
26. Accounts Allowed to Dial In through RAS	120	
27. Services and Drivers on the Machine	131	
28. Security Updates, Patches and Hot-Fixes	143	
29. Current Network Connections	144	
30. Logical Drives	145	
31. Network Shares	148	
32. Home Directories, Logon Scripts and Profiles		
33. File Permissions and Auditing		

This picture shows the content of a SekChek for Windows report.

The report contains more than 40 sub-sections spanning all aspects of security for an entire Active Directory domain.

For example, reports include:

- Domain-wide policies, such as password lengths and intruder detection settings
- Audit log settings, which indicate the type of events being logged by your system
- Exception reports for all user and group objects, which highlight high risk accounts that do not comply with your security standards
- Group policy objects and settings linked to Organizational Units and Sites
- FSMO roles held by domain controllers on your system
- The status of services and drivers running on the system
- Installed hot-fixes and service packs
- Access permissions defined on sensitive files, directories and registry keys

# A Quick Tour of a SekChek Report: 4 of 8

## Multiple reporting levels...



The picture illustrates the multiple reporting levels provided by SekChek.

The chart provides a convenient and easy-to-read summary of the most important properties defined on security objects on your system. It provides a high level view of security and uses colour to indicate whether a specific control is above or below the average for your industry sector.

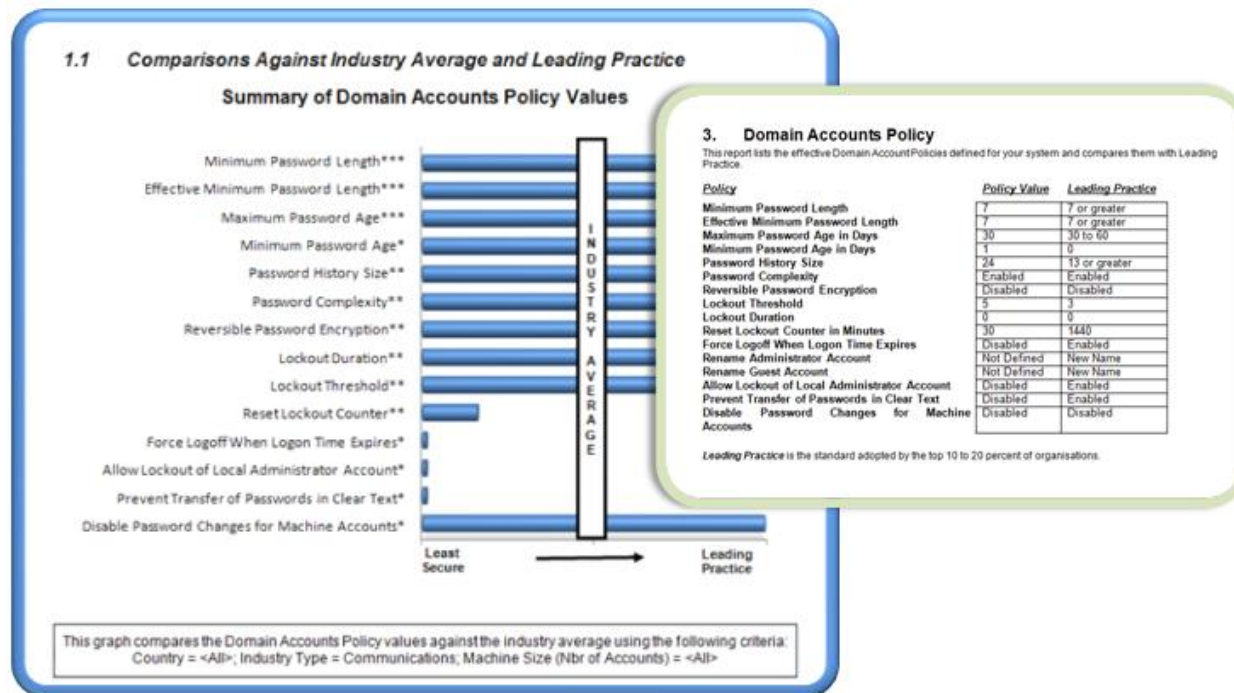
The text-based summary provides the numbers behind the percentages on the chart for various categories of account. Examples include values for all user accounts, active accounts only and separate reports that isolate higher risk Administrative accounts.

Of course, SekChek's high level summaries are supported by comprehensive detailed reports presented in a familiar tabular style in MS-Word, Excel or Access file formats.

The detailed reports provide the information you need to identify exceptions and specific weaknesses, so you can take the necessary corrective action to correct the problem.

# A Quick Tour of a SekChek Report: 5 of 8

## System-wide security policies...



This picture illustrates the different ways that SekChek presents system-wide policy settings.

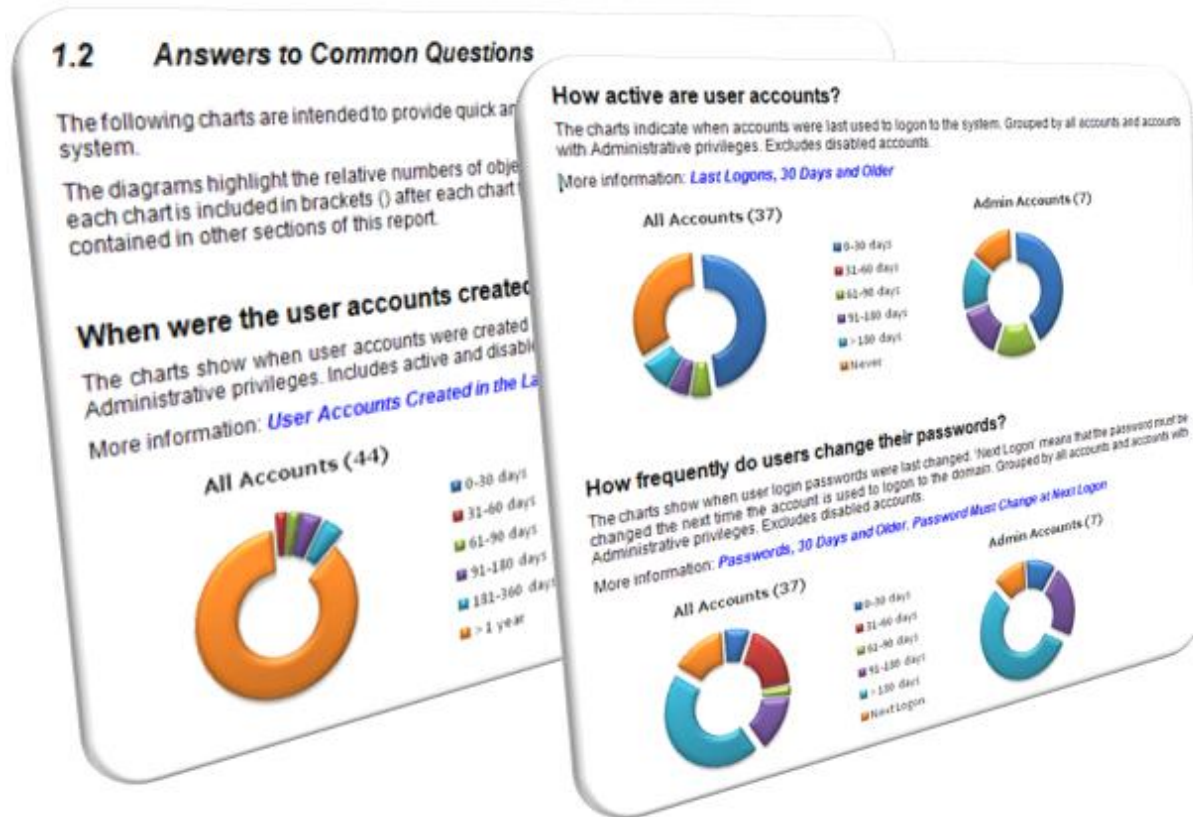
The summary chart provides a quick and easy-to-read assessment of the strength of your system-wide policies, including how those policies compare against those used on similar types of system employed by your industry peers.

Certain policies only have two possible settings (on or off), while other policies can be set to any value within a predefined range.

SekChek's summary graphs are supported by detailed reports, which compare a policy's current setting against the leading practice for the control that is implemented by other organisations in your particular industry sector.

# A Quick Tour of a SekChek Report: 6 of 8

## Quick answers to common questions...



This report section provides you with quick answers to the most common questions about security.

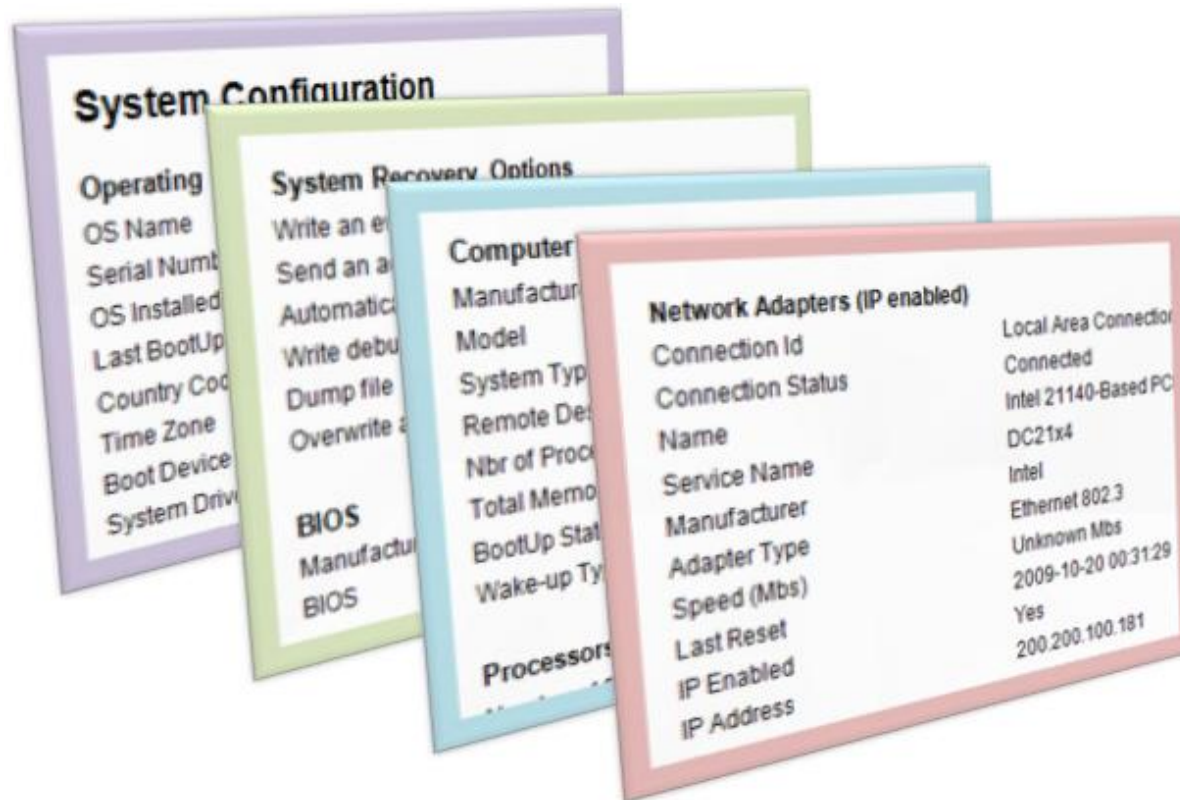
The pie charts typically exclude accounts that do not pose an immediate threat to security because they have been disabled by an Administrator or locked by the system. As such, they provide a perspective of security that is closer to *real risk*, rather than measuring a deviation from a security standard.

The charts also present separate views for normal, regular user accounts and higher risk accounts with administrative privileges.

If an account property is not replicated across domain controllers, SekChek provides an option to query *all* domain controllers, so you can view the property's latest and most current value.

# A Quick Tour of a SekChek Report: 7 of 8

## System configuration settings...



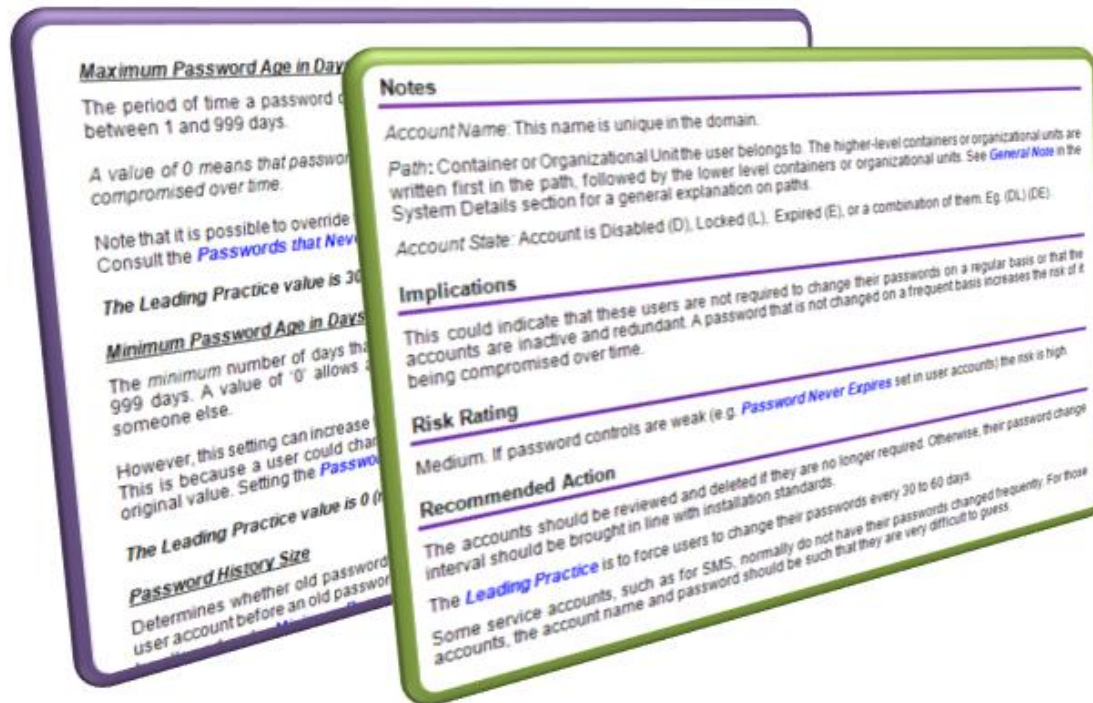
In addition to security-related controls, SekChek also analyses many system configuration and hardware-related settings.

Some examples include:

- Information about the OS and computer, such as the system's time zone, serial number, manufacturer, service pack, BIOS version and last boot-up time
- System recovery options, which control how the system will respond in the event of a hardware or software failure
- Hardware specifications and features supported by a system's disk drives, network adapters and processors (CPUs)
- Speed and resource availability settings, such as the available free space on disk volumes and the current and maximum sizes of page files and virtual memory

# A Quick Tour of a SekChek Report: 8 of 8

## Explanations, Implications, Risk Ratings, Recommendations...



This last picture illustrates how SekChek reports can help you to quickly understand and respond to exceptions and weaknesses highlighted by your report.

Each section of your report contains details of: Implications; a Risk Rating; and Recommended Actions.

Implications – explain why a control is important and how it impacts on the security of your system.

Risk Ratings – indicate the importance of the control relative to other security controls.

Recommended Actions – provide you with useful advice and actions you should take to address weaknesses in your controls.

This concludes the brief tour of a SekChek report.

Please let us know if you have any questions. You are also welcome to download the sample reports on our web site.